## CLAIMS

What is claimed is:

1. A computerized method comprising:

determining an active networked application;

filtering a set of intrusion rules to create a subset of rules corresponding to the active networked application; and

evaluating network traffic using the subset of rules.

2. The computerized method of claim 1 further comprising:

detecting when the active networked application becomes inactive; and

re-filtering the set of intrusion rules.

3. The computerized method of claim 2, wherein the detecting comprises:

monitoring network connection terminations.

4. The computerized method of claim 2, wherein the detecting comprises:

monitoring application terminations.

5. The computerized method of claim 1 further comprising:

detecting when no networked application is active; and

suspending the evaluating of network traffic until a networked application is active.

6. The computerized method of claim 1, wherein the subset of rules further corresponds to an operating system and further comprising:

continuing the evaluating of network traffic if no networked application is active.

7. The computerized method of claim 1, wherein the determining comprises:

detecting when a network connection for an active application is initiated.

8. The computerized method of claim 1, wherein the filtering comprises:

marking an intrusion rule corresponding to the active networked application.

9. The computerized method of claim 1, wherein the filtering comprises:

extracting the subset of rules into an optimized set of rules.

10. The computerized method of claim 1, wherein the evaluating comprises:

analyzing network traffic on a port specified in the subset of rules.

11. The computerized method of claim 1, wherein the evaluating comprises:

analyzing network traffic for a protocol specified in the subset of rules.

12. The computerized method of claim 1, wherein the evaluating comprises:

discarding network traffic that satisfies at least one of the subset of rules; and

reporting an intrusion attempt.

13. The computerized method of claim 1, wherein the set of intrusion rules comprises signatures of known attacks.

14. The computerized method of claim 1, wherein the set of intrusion rules comprises heuristic rules.

15. A computer-readable medium having executable instructions to cause a computer to perform a method comprising:

determining an active networked application;

filtering a set of intrusion rules to create a subset of rules corresponding to the active networked application; and

evaluating network traffic using the subset of rules.

16. The computer-readable medium of claim 15, wherein the method further comprises:

detecting when the active networked application becomes inactive; and

re-filtering the set of intrusion rules.

17. The computer-readable medium of claim 16, wherein the detecting comprises:

monitoring network connection terminations.

18. The computer-readable medium of claim 16, wherein the detecting comprises:

monitoring application terminations.

19. The computer-readable medium of claim 15, wherein the method further comprises:

detecting when no networked application is active; and

suspending the evaluating of network traffic until a network application is active.

20. The computer-readable medium of claim 15, wherein the subset of rules further corresponds to an operating system and the method further comprises:

continuing the evaluating of network traffic if no networked application is active.

21. The computer-readable medium of claim 15, wherein the determining comprises:

detecting when an active application initiates a network connection.

22. The computer-readable medium of claim 15, wherein the filtering comprises:

marking an intrusion rule corresponding to the active networked application.

23. The computer-readable medium of claim 15, wherein the filtering comprises:

extracting the subset of rules into an optimized set of rules.

24. The computer-readable medium of claim 15, wherein the evaluating comprises:

analyzing network traffic on a port specified in the subset of rules.

25. The computer-readable medium of claim 15, wherein the evaluating comprises:

analyzing network traffic for a protocol specified in the subset of rules.

26. The computer-readable medium of claim 15, wherein the evaluating comprises:

discarding network traffic that satisfies at least one of the subset of rules; and

reporting an intrusion attempt.

27. The computer-readable medium of claim 15, wherein the set of intrusion rules comprises signatures of known attacks.

28. The computer-readable medium of claim 15, wherein the set of intrusion rules comprises heuristic rules.

29. A system comprising:

a processor coupled to a memory through a bus; and

an intrusion prevention process executed from the memory by the processor to cause the processor to determine an active networked application, to filter a set of intrusion rules to create a subset of rules corresponding to the active networked application, and to evaluate network traffic using the subset of rules.

30. The system of claim 29, wherein the intrusion prevention process further causes the processor to detect when the active networked application becomes inactive, and to re-filter the set of intrusion rules.

31. The system of claim 30, wherein the intrusion prevention process further causes the processor to monitor network connection terminations in detecting when the active networked application becomes inactive.

32. The system of claim 30, wherein the intrusion prevention process further causes the processor to monitor application terminations in detecting when the active networked application becomes inactive.

33. The system of claim 29, wherein the intrusion prevention process further causes the processor to detect when no networked application is active, and to suspend evaluating network traffic until a network application is active.

34. The system of claim 29, wherein the intrusion prevention process further causes the processor to further filter the intrusion rules based on an operating system and to continue evaluating network traffic if no networked application is active.

35. The system of claim 29, wherein the intrusion prevention process further causes the processor to detect when an active application initiates a network connection in determining an active networked application.

36. The system of claim 29, wherein the intrusion prevention process further causes the processor to mark an intrusion rule corresponding to the active networked application in filtering the set of intrusion rules.

37. The system of claim 29, wherein the intrusion prevention process further causes the processor to extract the subset of rules into an optimized set of rules in filtering the set of intrusion rules.

38. The system of claim 29, wherein the intrusion prevention process further causes the processor to analyze network traffic on a port specified in the subset of rules in evaluating the network traffic.

39. The system of claim 29, wherein the intrusion prevention process further causes the processor to analyze network traffic for a protocol specified in the subset of rules in evaluating the network traffic.

40. The system of claim 29, wherein the intrusion prevention process further causes the processor to discard network traffic that satisfies at least one of the subset of rules, and to report an intrusion attempt in evaluating the network traffic.

41. The system of claim 29, wherein the set of intrusion rules comprises signatures of known attacks.

42. The system of claim 29, wherein the set of intrusion rules comprises heuristic rules.

43. An apparatus comprising:

means for determining when an active application becomes an active networked application;

means for filtering coupled to the means for determining to create a subset of rules corresponding to the active networked application from a set of intrusion rules; and

means for evaluating coupled to the means for filtering to evaluate network traffic using the subset of rules.

44. The apparatus of claim 43, wherein the means for determining further detects when the active networked application becomes inactive and the means for filtering further re-filters the set of intrusion rules when the active networked application becomes inactive.

45. The apparatus of claim 43, wherein the means for determining further detects when no networked application is active and the means for evaluating further suspends the evaluation of network traffic until the means for determining determines a networked application is active.

46. The apparatus of claim 43, wherein the means for filtering further filters the intrusion rules corresponding to an operating system and the means for evaluating continues the evaluation of network traffic when the means for determining determines no networked application is active.

47. The apparatus of claim 43, wherein the means for evaluating comprises:

means for discarding network traffic that satisfies at least one of the subset of rules; and

means for reporting an intrusion attempt.